Qphone: A Quantum Security VoIP Phone

Bo Liu
School of Computer
National University of Defense Technology
Changsha, Hunan, China
liub0yayu@gmail.com

Baokang Zhao
School of Computer
National University of Defense Technology
Changsha, Hunan, China
bkzhao@nudt.edu.cn

Ziling Wei
School of Computer
National University of Defense Technology
Changsha, Hunan, China
wzl1017@gmail.com

Chunqing Wu
School of Computer
National University of Defense Technology
Changsha, Hunan, China
cqwu@nudt.edu.cn

Jinshu Su
School of Computer
National University of Defense Technology
Changsha, Hunan, China
sjs@nudt.edu.cn

Wanrong Yu
School of Computer
National University of Defense Technology
Changsha, Hunan, China
ywrong@gmail.com

Fei Wang
School of Computer
National University of Defense Technology
Changsha, Hunan, China
wangfei85@gmail.com

Shihai Sun
Department of Physics
National University of Defense Technology
Changsha, Hunan, China
shsun@nudt.edu.cn

ABSTRACT

This work presents a novel quantum security VoIP phone, called Qphone. Qphone integrates quantum key distribution (QKD) and VoIP steganography, and achieves peer-to-peer communication with information-theoretical security (ITS) guaranteeing. Qphone consists of three parts, a real-time QKD system, RT-QKD, a steganography software, VS-Phone, and an audio encryption and authentication hardware, AE-KEY. RT-QKD explores QKD technologies, and is able establish a shared key between two peers ensuring ITS. VS-Phone utilizes VoIP steganography to protect transmission channels of sensitive information. Qphone can provide efficient and real-time security protections to meet different security demands.

Categories and Subject Descriptors

C.2.0 [Computer Communication Networks]: Security and protection

General Terms

Measurement, Design, Experimentation, Security

Keywords

Quantum Communication, VoIP, steganography, security

1. INTRODUCTION

Quantum Key Distribution (QKD) [1] technology is an important practical application of quantum information. QKD system, based on laws of physics rather than computational complexity of mathematical problems, can create information-theoretical security (ITS) keys between communication parties. With the ITS keys, we can protect the security of the sensitive content with one-time pad, AES and other security protection schemes.

SIGCOMM'13, Aug 12-16 2013, Hong Kong, China
ACM 978-1-4503-2056-6/13/08.

Since information transmission channel is public on the internet, attackers may detect and modify our encrypted sensitive content. If we want to share sensitive information on extremely unsafe network, the transmission channel must be well protected.

Streaming steganography is able to protect the security of sensitive information transmission channels with the capability of hide sensitive information within online streams. For example, we can hide our sensitive information into VoIP streams.

Integrating QKD and VoIP steganography technology, we design and develop Qphone, a novel quantum security VoIP phone. Qphone is a hardware/software co-designed system with real-time processing capabilities. It consists of three parts, RT-QKD, VS-Phone and AE-Key. RT-QKD is a real-time QKD system. VS-Phone is the VoIP steganography software. AE-Key is the audio encryption and authentication hardware.

Qphone can provide efficient security protection to meet different security demands. Generally, Qphone provides high-speed security application by encrypting VoIP streams with AES method before the streams are transmitted on the Internet. When the network suffers serious security threats, Qphone can provide low-speed security application, such as Instant Messaging (IM), by encrypting information with OTP method and hiding information into VoIP streams.

2. AN OVERVIEW OF QPHONE

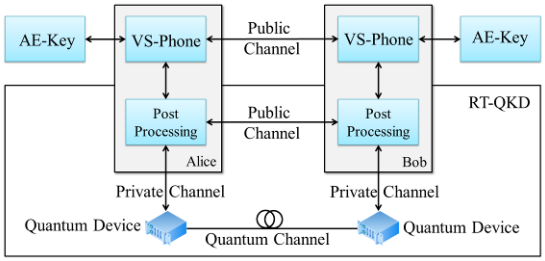


Figure 1: The Architecture of Qphone

As shown in Figure 1, Our Qphone system consists of three parts, RT-QKD, VS-Phone and AE-Key.

RT-QKD is a real-time QKD system, which generates ITS keys for communication parties. The communication distance of RT-

QKD system reaches 25 km. Our RT-QKD system conducts BB84 protocol. The quantum bit error rate of RT-QKD system is lower than 5%. In this paper, we use the quantum communication system proposed in our previous work [3].

RT-QKD involves two phases, quantum communication phase and classical post-processing phase. In quantum communication phase, Alice and Bob exchange quantum information with each other through quantum devices. Based on our previous work in [2-5], we design a real-time post-processing scheme. Post-processing modules connect with each other through public channels and connect to quantum devices through local private channels. They gain quantum information from quantum devices. With the efficient error correction technology based on low-density parity-check code and privacy amplification technology based on Toeplitz matrix, post-processing modules can generate ITS keys. The final security key rate of RT-QKD is about 2kb/s.

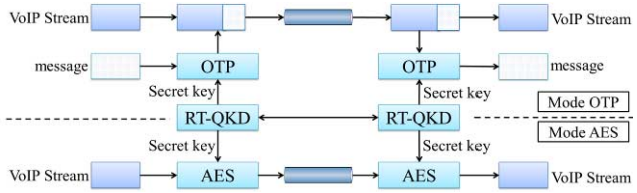
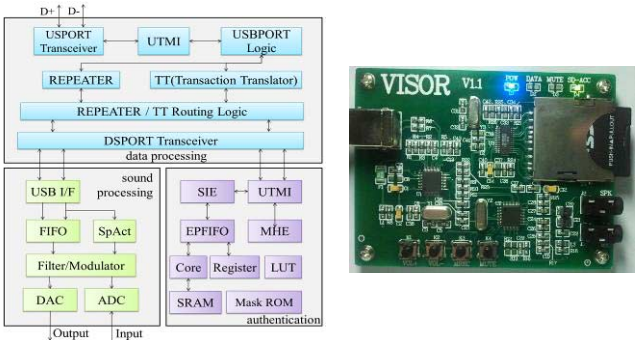


Figure 2: The working modes of VS-Phone



(a) **(b)**

Figure 3: (a) structure of AE-Key, (b) hardware of AE-Key

VS-Phone is the supporting software for VoIP steganography. In VS-Phone, we implement the steganography chatting application. It works in two modes OTP and AES, as shown in Figure 2. For low-speed network applications, such as IM, VS-Phone gains secret keys from RT-QKD system, encrypts messages by OTP method and then hides encrypted information into VoIP streams. It's the highest level security protection. For high-speed network applications, such as online telephone, VS-Phone provides AES encrypted protection with the key length of 1024 bits. The key refreshes per minute. In our previous work [5], we have proposed Adaptive VoIP Steganography (AVIS) scheme which enhances the anti-detecting and anti-attacking ability of VoIP steganography.

As shown in Figure 3, AE-Key enhances the security of Qphone by hardware authentication and audio encryption. It consists of sound processing module, authentication module and data processing module. In the authentication module, users need to insert their ID chips to get the access to VS-Phone. In the sound processing module, all audio input and output are converted, filtered and modulated in case that attackers use Trojan or malwares to eavesdrop on internal sound system.

As we shown before, the proposed Qphone can provide efficient security protection for sensitive content and transmission channels. It provides different security services for both low-speed and high-speed network applications (such as IM and online telephone).

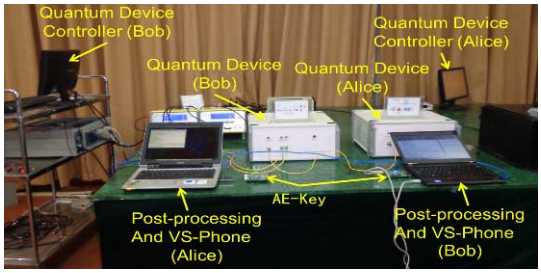


Figure 4: The experiment environment of Qphone

3. DEMO DESCRIPTION

The experiment environment of our demo is shown in Figure 4. There will be three procedures in our demo. Firstly, we will illustrate how RT-QKD generates ITS keys without steganography procedures. Secondly, we will use the AVIS steganography mechanism to illustrate how VoIP steganography works. Finally, we will start RT-QKD, VS-Phone and AE-Key at the same time to validate system performance over various interferences.

4. ACKNOWLEDGEMENT

The work described in this paper is supported by the project of National Science Foundation of China under grant No.61202488, the program for Changjiang Scholars and Innovative Research Team in University (No.IRT1012).

5. REFERENCES

[1] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Vol. 175. No. 0. Bangalore, India, 1984.

[2] Liu, Bo, et al. "A Real-Time Privacy Amplification Scheme in Quantum Key Distribution." *Information and Communication Technology*. Springer Berlin Heidelberg, 2013. 453-458.

[3] Sun S H, Ma H Q, Han J J, et al. Quantum key distribution based on phase encoding in long-distance communication fiber. *Optics letters*, 2010, 35(8): 1203-1205.

[4] Zou, Dingjie, et al. "CLIP: A Distributed Emulation Platform for Research on Information Reconciliation." *Network-Based Information Systems (NBiS), 2012 15th International Conference on*. IEEE, 2012.

[5] Wei, Ziling, et al. "VISOR: A Practical VoIP Steganography Platform." *Mobile Ad-hoc and Sensor Networks (MSN), 2011 Seventh International Conference on*. IEEE, 2011.